UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/618,202 | 07/18/2000 | Kenji Yamagami | 16869C008600US | 9713 |

7590 07/19/2006

Robert C Colwell
Townsend and Townsend and Crew LLP
8th Floor
Two Embarcadero Center
San Francisco, CA 94111-3834

| EXAMINER | |
|---|---|
| HOFFMAN, BRANDON S | |
| **ART UNIT** | **PAPER NUMBER** |
| 2136 | |

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/618,202 | YAMAGAMI ET AL. | |
| | Examiner | Art Unit | |
| | Brandon S. Hoffman | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *14 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-11,13-22,26,27 and 30-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,13-22,26,27 and 30-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-11, 13-22, 26, 27, and 30-32 are pending in this office action.

2. Applicant's arguments, filed April 14, 2006, have been considered and are persuasive. However, a new ground of rejection is made.

### *Rejections*

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### *Claim Rejections - 35 USC § 103*

4. Claims 1-11, 13-22, 26, 27, and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohran (U.S. Patent No. 6,397,307) in view of Yanai et al. (U.S. Patent No. 5,544,347), and further in view of Matsui et al. (U.S. Patent No. 6,742,116).

Regarding claims 1, 2, 17, 18, and 30-32, Ohran as modified by Yanai et al. teaches a method of controlling security of data in a storage system having a local disk system and a remote disk system that are coupled to at least one host computer, the method comprising:

- In the local disk system coupled to a first host computer:
    - When a write of data is to be made to the local disk system retrieving the first encryption key (see col. 11, lines 24-26 of Ohran suggests to use

stored encryption keys for encryption, even though the teachings of Ohran dynamically creates an encryption key);

- Encrypting the data (see col. 11, lines 43-45 of Ohran);
- Transferring the encrypted data to the remote disk system via a first communication link (see col. 11, lines 45-47 of Ohran);

- Then in the remote disk system:
  - Determining an address for storage of the data in the remote disk system (se col. 9, lines 29-35 and col. 10, lines 21-27 of Ohran);
  - Determining whether the data is to be stored in an encrypted form **or a decrypted form** (see col. 11, lines 40-43 of Ohran suggests that some of the data can be encrypted, but does not necessarily mean the same data has to be decrypted); and
  - If the data is to be stored in a decrypted form, decrypting and writing the data in the remote disk system (see col. 11, lines 47-49 of Ohran); and
  - If the data is to be stored in an encrypted form, writing the data in the remote disk system without decrypting the data (see col. 11, lines 40-43 of Ohran, the word ***may*** suggests that the data does not have to be decrypted),
  - notifying the local disk system that the step of writing the data is complete (see col. 6, lines 41-46 of Yanai et al.),
- Wherein the local disk system is coupled to the first host computer via a second communication link to allow the first host computer to access data stored in the

local disk system, the first and second communication links being different (see fig. 1, ref. num 40 and 18 of Yanai et al.),

- Wherein the data transfer between the local disk system and the remote disk system occurring via a communication link that couples the local disk system to the remote disk system, so that the local disk system may send the data to the remote disk system without direct involvement from the host computer (see fig. 1, ref. num 16 of Ohran, col. 5, lines 53-63 of Yanai et al., and col. 6, lines 16-37 of Yanai et al.),
- Wherein the list of encryption keys includes first and second keys, the first key being assigned to a first set of volumes in the local disk system, and the second key being assigned to a second set of volumes in the local disk system, each of the first and second set of volumes including one or more volumes (see col. 11, lines 53-55 of Ohran),
- Wherein the remote disk system is coupled to a second host computer (see fig. 1, ref. num 52 and 54 of Yanai et al.).

However, the combination of Ohran as modified by Yanai et al. does not teach further comprising a step of maintaining an encryption control table on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system, wherein the retrieving step includes accessing the encryption control table to obtain an appropriate encryption key, where the data are encrypted using the first key if the data to be transferred to the remote disk

system are associated with the first set of volumes and encrypted using the second key if the data to be transferred to the remote disk system are associated with the second set of volumes.

Matsui et al. teaches further comprising a step of maintaining an encryption control table on the local disk system (fig. 7), the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system (fig. 7, INDEX), wherein the retrieving step includes accessing the encryption control table to obtain an appropriate encryption key, where the data are encrypted using the first key if the data to be transferred to the remote disk system are associated with the first set of volumes and encrypted using the second key if the data to be transferred to the remote disk system are associated with the second set of volumes (col. 11, lines 5-37).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine maintaining an encryption control table on the local disk system wherein the table includes a list of encryption keys for selected volumes of the local and remote disk system, as taught by Matsui et al., to the system of Ohran as modified by Yanai et al. It would have been obvious for such modifications because the table provides a list of keys to use for encryption and decryption for the local remote system. This new system uses a table of keys to determine how and when to encrypt and decrypt the data in the local and remote system.

Regarding claims 3 and 19, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the local disk system (see col. 11, lines 40-43 of Ohran suggests that encryption/decryption can occur, but does not have to occur and col. 5, lines 9-16 of Matsui et al.).

Regarding claims 4 and 20, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the remote disk system (see col. 11, lines 40-43 of Ohran and col. 5, lines 9-16 of Matsui et al.).

Regarding claims 5 and 21, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the encryption key is applicable to less than all of the storage on the local disk system (see col. 11, lines 40-43 of Ohran shows that some, less than all, of the data is encrypted).

Regarding claims 6 and 22, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the encryption key is applicable to less than all of the storage on the remote disk system (see col. 11, lines 43 of Ohran shows that some, less than all, of the data is decrypted).

Regarding claim 7, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the encryption key is applicable to at least one disk on the local disk system (see col. 11, lines 40-43 of Ohran and fig. 1, ref. num 20 of Yanai et al. shows that the different volumes would not have to be encrypted, such as the local volume, because transmission does not occur from the local volume).

Regarding claim 8, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the encryption key is applicable to at least one disk on the remote disk system (see col. 11, lines 40-43 of Ohran and fig. 1, ref. num 48 of Yanai et al. shows that the different volumes would not have to be decrypted, such as the local volume, because transmission does not occur to the local volume).

Regarding claims 9 and 13, Ohran as modified by Yanai et al. teaches a method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

- Determining a boundary in the local disk system where encryption is to be switched to an opposite state (see col. 11, lines 52-55 of Ohran, the keys are changed at every time of consolidation);
- In the remote disk system receiving a corresponding boundary from the remote disk system (see col. 6, lines 16-37 of Yanai et al., the remote system boundary is the same place that the local system boundary is);

- In both the local and the remote disk system, determining a relationship of present operations to the boundary (see fig. 2, ref. num 30, 36, and 42 of Ohran);
- In both the local and the remote disk system waiting for the boundary, and then changing the encryption to the opposite state (see fig. 2, ref. num 32 and 38 of Ohran),
- Wherein the local disk system is coupled to a host computer via a first communication link, and the remote disk system is coupled to a second host computer via a second communication link, the local disk system and the remote disk system being coupled to each other via a third communication link, the third communication link being different than the first or second communication link (see fig. 1, ref. num 18, 40, 52, and 54 of Yanai et al.)

However, the combination of Ohran as modified by Yanai et al. does not teach maintaining a control table in each of the local and remote disk systems.

Matsui et al. teaches maintaining a control table in each of the local and remote disk systems (fig. 7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine maintaining a control table in each of the the local disk system and the remote disk system, as taught by Matsui et al., to the system of Ohran as modified by Yanai et al. It would have been obvious for such modifications because

the table provides a list of keys to use for encryption and decryption for the local remote system. This new system uses a table of keys to determine how and when to encrypt and decrypt the data in the local and remote system.

Regarding claim 10, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein operations before the boundary are performed using a first encryption key and operations after the boundary are performed using a second encryption key (see col. 11, lines 52-55 of Ohran).

Regarding claims 11 and 15, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein the boundary is defined by counting input/output operations and using the count to define the boundary (see col. 13, lines 35-50 of Ohran uses a decided time T to decide the boundary, and only the last IO operation before a decided time T is transmitted to the remote system).

Regarding claim 14, the combination of Ohran and Yanai et al. as modified by Matsui et al. teaches wherein operations before the boundary are either encrypted or not encrypted, and operations performed after the boundary are either not encrypted or encrypted oppositely to those operations performed before the boundary (see col. 11, lines 40-43 of Ohran, the data can be encrypted at any time and can not be encrypted anytime, it all depends on the users' data).

Regarding claims 16 and 26, Ohran as modified by Yanai et al. teaches a method/system of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

- The first and second encryption keys assigned to first and second volumes of the local disk system, respectively (see fig. 1, ref. num 22a, 22b, 50a, 50b of Yanai et al.);
- Transmitting via a second communication link the first and second encryption key to the remote disk system and storing it in a memory there (see fig. 6, ref. num 16 and 106b of Ohran), the remote disk system including third and fourth volumes corresponding to the first and second volumes, respectively (see fig. 1, ref. num 22a, 22b, 50a, 50b of Yanai et al.);
- Splitting the local disk system from the remote disk system to allow them to operate independently (see fig. 2 of Ohran, the time between consolidations the local system is operated independently of the remote system), wherein the splitting is performed according to a first command issued by the local or remote disk system (see col. 6, lines 16-37 of Yanai et al.);
- Switching encryption to an opposite state from a previous state after splitting the local disk system and remote disk system (see col. 11, lines 40-43 of Ohran, the data can be encrypted at any time and can not be encrypted anytime, it all depends on the users' data); and
- Re-synchronizing the local disk system and the remote disk system (see col. 6, lines 38-51 of Yanai et al.), wherein the re-synchronizing is performed according

to a second command issued by the local or remote disk system (see col. 7, lines 13-31 of Yanai et al.), the first and second communication links being different (see fig. 1, ref. num 18 and 40 of Yanai et al.).

However, the combination of Ohran as modified by Yanai et al. does not teach storing first and second encryption keys in a memory in the local disk system that is coupled to a host computer via a first communication link.

Matsui et al. teaches storing first and second encryption keys in a memory in the local disk system that is coupled to a host computer via a first communication link (fig. 7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine storing first and second encryption keys in a memory in the local disk system that is coupled to a host computer via a first communication link, as taught by Matsui et al., to the system of Ohran as modified by Yanai et al. It would have been obvious for such modifications because the index and common key identifies which key should be used in a system where there are multiple computers.

Regarding claim 27, Ohran as modified by Yanai et al. teaches a method of controlling security of data in a storage system having a local disk system and a remote disk system comprising:

- In the local disk system, the local disk system including first and second volumes (see fig. 1, ref. num 22a, 22b, 50a, 50b of Yanai et al.):
    - Receiving a data update request from a host computer connected to the local disk system wherein said data update request includes a location of the first volume of the local disk system, the host computer being connected to the local disk via a first communication link (see col. 5, lines 39-52 of Ohran, the local disk system is required to determine update times and fig. 1, ref. num 22a of Yanai et al.);
    - Transferring the encrypted data to the remote disk system (see col. 11, lines 45-47 of Ohran);
- Then in the remote disk system:
    - Decrypting the data using the first key (see col. 11, lines 47-49 of Ohran); and
    - Writing the decrypted data into a third volume of the remote disk system by the remote disk system (see col. 9, lines 39-43 and col. 10, lines 21-27 of Ohran),
- Wherein the first and second communication links are different (see fig. 1, ref. num 18 and 40 of Yanai et al.).

However, the combination of Ohran as modified by Yanai et al. does not teach the first and second volumes are assigned first and second encryption keys or

encrypting the data associated with the first volume of the local disk system using the first key.

Matsui et al. teaches the first and second volumes are assigned first and second encryption keys (fig. 7) and encrypting the data associated with the first volume of the local disk system using the first key (fig. 7, INDEX).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the first and second volumes are assigned first and second encryption keys and encrypting the data associated with the first volume of the local disk system using the first key, as taught by Matsui et al., to the system of Ohran as modified by Yanai et al. It would have been obvious for such modifications because the index and common key identifies which key should be used in a system where there are multiple computers.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100